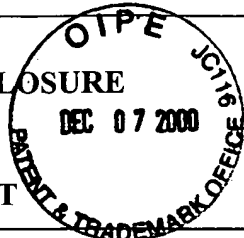


**INFORMATION DISCLOSURE  
STATEMENT**

**BY APPLICANT**



Docket: 245-55512

App: 09/637,229

Applicant: Çetin K. Koç et al.

Filed: August 11, 2000

Art Unit: 2766

**OTHER DOCUMENTS**

<i>mv</i>			Kaliski, Jr., B.S., "The Montgomery Inverse and Its Applications," <u>IEEE Trans. on Computers</u> 44:1064-1065 (August 1995)
<i>mv</i>			Montgomery, P.L., "Modular Multiplication Without Trial Division," <u>Math. of Computation</u> 44:519-521 (April 1985)
<i>mv</i>			Koç, Ç.K. et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," <u>IEEE Micro</u> 16:26-33 (June 1996)
<i>mv</i>			Dhem, J. et al., "SCALPS: Smart Card For Limited Payment Systems," <u>IEEE Micro</u> 16:42-51 (June 1996)
<i>mv</i>			Diffie, W., Hellman, M.E., "New Directions in Cryptography," <u>IEEE Trans. on Information Theory</u> 22:644-654 (1976)
<i>mv</i>			Rivest, R.L. et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," <u>Communications of the ACM</u> 21:120-126 (1978)
<i>mv</i>			Koç, Ç.K., Acar, T., "Fast Software Exponentiation in $GF(2^k)$ " in <u>Proceedings, 13<sup>th</sup> Symposium on Computer Arithmetic</u> , pp. 225-231 (July 1997) (T. Lang et al., editors)
<i>mv</i>			Hamano, T. et al., " $O(n)$ -Depth Circuit Algorithm for Modular Exponentiation" in <u>Proceedings, 12th Symposium on Computer Arithmetic</u> , pp. 188-192 (July 1995) (S. Knowles, W.H. McAllister, editors)
<i>mv</i>			Orup, H., "Simplifying Quotient Determination in High-radix Modular Multiplication" in <u>Proceedings, 12th Symposium on Computer Arithmetic</u> , pp. 193-199 (July 1995) S. Knowles, W.H. McAllister, editors)

EXAMINER:

*Michael D. Chung*

DATE

2-26-04

\*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.

**RECEIVED**

DEC 11 2000

Technology Center 2100

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>			Docket: 245-55512	App: 09/637,229
			Applicant: Çetin K. Koç et al.	
			Filed: August 11, 2000	Art Unit: 2766
<b>OTHER DOCUMENTS</b>				
<i>mv</i>			Bernal, A., Guyot, A., "Design of a Modular Multiplier Based on Montgomery's Algorithm" in <u>13<sup>th</sup> Conference on Design of Circuits and Integrated Systems</u> , pp. 680-685 (November 1998)	
<i>mv</i>			Eldridge, S.E., Walter, C.D., "Hardware Implementation of Montgomery's Modular Multiplication Algorithm," <u>IEEE Trans. Computers</u> 42:693-699 (June 1993)	
<i>mv</i>			Kornerup, P., "High-Radix Modular Multiplication for Cryptosystems" in <u>Proceedings, 11th Symposium on Computer Arithmetic</u> , pp. 277-283 (June 1993) (E. Swartzlander et al., editors)	
<i>mv</i>			Walter, C.D., "Space/Time Trade-offs for Higher Radix Modular Multiplication Using Repeated Addition," <u>IEEE Trans. Computers</u> 46:139-141 (1997)	
<i>mv</i>			Royo, A., et al., "Design and Implementation of a Coprocessor for Cryptography Applications," <u>European Design and Test Conference</u> , pp. 213-217 (March 1997)	
<i>mv</i>			Koç, Ç.K., Acar, T., "Montgomery Multiplication in GF(2k), " <u>Designs, Codes and Cryptography</u> 14:57-69 (1998)	
<i>mv</i>			Tenca, A.F., "Variable Long-Precision Arithmetic (VLPA) for Reconfigurable Coprocessor Architectures," Ph.D. Thesis, University of California at Los Angeles (March 1998)	
<i>mv</i>				
<i>mv</i>				
EXAMINER: <i>Michael Vay</i>			DATE <i>2-26-04</i>	
*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.			<b>RECEIVED</b> DEC 11 2000	

**RECEIVED**

JUL 0 5 2002

App: 09/637,229

Technology Center 2100

**INFORMATION DISCLOSURE  
STATEMENT**

Docket: 245-55512

Applicant: Koc et al.

**BY APPLICANT**

Filed: August 11, 2000

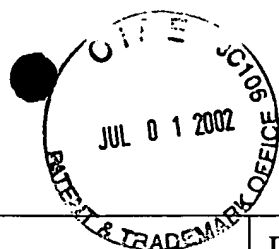
Art Unit:

**U.S. PATENT DOCUMENTS**

Init.*		Number	Date	Name	Class	Sub	Filed
<i>mv</i>		6,151,393	11/21/00	Jeong			
<i>mv</i>		5,742,530	4/21/98	Gressel et al.			
<i>mv</i>		6,049,815	4/11/00	Lambert et al.			
<i>mv</i>		6,035,317	3/7/00	Guy			
<i>mv</i>		5,867,412	2/2/99	Suh			
<i>mv</i>		6,209,016 B1	3/27/01	Hobson et al.			
<i>mv</i>		5,745,398	4/28/98	Monier			
<i>mv</i>		5,144,574	9/1/92	Morita			
<i>mv</i>		5,513,133	4/30/96	Cressel et al.			
<i>mv</i>		6,185,596 B1	2/6/01	Hadad et al.			
<i>mv</i>		5,349,551	9/20/94	Petro			
<i>mv</i>		6,182,104 B1	1/30/01	Foster et al.			
<i>mv</i>		5,954,788	9/21/99	Suh et al.			

**OTHER DOCUMENTS**

<i>mv</i>			Hong et al., "New Modular Multiplication Algorithms for Fast Modular Exponentiation," EUROCRYPT '96 Proceedings, 166-177
-----------	--	--	--



MJ:mgs 06/25/2002 245-55512 124269

<b>INFORMATION DISCLOSURE STATEMENT</b>  <b>BY APPLICANT</b>			Docket: 245-55512	App: 09/637,229
			Applicant: Koc et al.	
			Filed: August 11, 2000	Art Unit:
<i>m</i>			Walter, C., "Faster Modular Multiplication by Operand Scaling," Advances in Cryptology Proc., Crypto '91, LNCS 576, 313-323 (1992)	
<i>m</i>			Even, S., "Systolic Modular Multiplication," Crypto 90 Proc. Lecture Notes in Computer Science no. 537, 619-624	
<i>m</i>			Bosselaers et al., "Comparison of Three Modular Reduction Functions," Crypto '94, 175.186	
EXAMINER: <i>Michael Chaf</i>			DATE <i>2-26-04</i>	
*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.				